6. INFORMATION OPERATIONS AND WARFARE

(Also see topics 3.40, and 3.62)

Doctrine, Definitions, and Conceptual Issues

6.1 Analyze the DOD role in protecting the United States National Information Infrastructure.

- Summarize existing national and DOD guidance (e.g. PDDs, national plans, DOD directives).
- Conduct a deficit analysis between infrastructure threats and existing protection programs.
- Analyze possible new approaches to protection of the national infrastructure, and how to address the threat.

Priority: 1
Key Terms: IO, IW, NII, Defending America's Cyberspace, Homeland Defense

6.2 What are the implications and issues surrounding IO and Homeland Defense?

- What are the areas of IO that could have a beneficial impact on Homeland Defense?
- What are the legal and ethical limits that must be taken into consideration?
- What are the proposed procedures for implementing an IO campaign within the Homeland Defense arena?

Priority: 1
Key Terms: IO, Homeland Defense

6.3 Are all Information Operations in essence Influence Operations with the common goal of gaining and maintaining Information Superiority?

- Does the AF IO Doctrine adequately define IO?
- What are the appropriate military elements of Influence Operations for AF/Joint Operations (Military Deception, PSYOP, OPSEC, PA, Civil Affairs)?
- Are Influence Operations more appropriately at the top of the hierarchy (of Information Operations) with Electronic Combat Operations (EW) and Network Operations (CNO) as subordinate mission areas within a measurable environment (Electromagnetic Spectrum and Cyberspace)?

Priority: 2
Key Terms: IO, IW, EW, CNO, EBO, C2W, OPSEC, Targeting, Influence Operations, ISR

6.4 Higher level IW effects are include actions to Destroy, Deny, Degrade, Disrupt, Deceive or Influence targets. What are key considerations that must be planned for to synchronize and deconflict those effects?

- What is the definition or unintended consequences or "blowback" in relation to IO actions?
- How can Intelligence Gain/Loss considerations be factored into the targeting process to best serve the needs of both ISR personnel and targeteers?
- What collateral damage considerations are unique to IW? Consider non-kinetic/non-lethal options.
- How important is the consideration of compromising a special capability to the IW campaign? Is their a risk-analysis model that can be applied to use of special capabilities to mitigate compromise?
- How can IW effects be embedded in the ATO to insure integration and to comply with the concept of parallel and simultaneous operations? Is the use of a "shadow" IO Tasking Order valid to protect use of IW capabilities, but to synchronize IW effects with kinetic ATO events?

Priority: 2
Key Terms: IO, IW, EBO, ATO, C2W, targeting, ISR, Influence Operations

6.5 What are the implications of arms control in the IW realm?

- How would an equitable arms control agreement be defined? What benefits might accrue? How are USAF equities protected?
- How are other IW powers' technological advances anticipated and addressed?
- What arms control mechanism(s) and forum/fora would be most appropriate for IW arms control? Is it possible to track/identify foreign IO/IW technology capabilities?
- How would the US Government identify, vet, and publish such a foreign "IW Militarily Critical Technologies List?" Given the short life cycle and rapid evolution of IO technologies, is this feasible given the existing bureaucratic processes?

Priority: 3
Key Terms: IO, IW, arms control, CNA, CND, IW agreements, critical technologies, proliferation

6.6 Should the US develop a declaratory policy regarding the use of its IW capabilities?

- Declaratory policies with respect to the use of nuclear, chemical and biological weapons exist in many forms that sometimes seem contradictory, (e.g., US has a no-use policy regarding CBW, but does not have a no first use policy regarding nuclear weapon).
- What specific lessons can IW learn from history with such policies for the use of NBC weapons? What facet of the weapons makes these lessons applicable to IO (e.g., controllability of effect, extent of collateral damage, risk of escalation, proliferation and technology transfer, force structure)?

- What national objectives can be best served by vagueness or explicitness on the subject of IW capabilities and our willingness to use them?
- How would such policies affect the contribution of IW to deterrence, both regionally and globally
- Should the US develop a national or DOD policy to limit a potential adversary's access to IW technologies? Assuming a critical technology list is available, how would verification and enforcement be done?

Priority: 3
Key Terms: IO, IW, Policy, SIOP, deterrence, first use, declaratory policies, critical technologies, proliferation, CNA, CND

6.7 How will evolving IO affect traditional deterrence and escalation dilemmas during international crises?

- What advantages does information dominance give during crisis negotiations?
- How have information advantages been used to intimidate crisis adversaries?
- Does information asymmetry make escalation to war more/less likely?
- Do evolving IO make it more/less difficult for civilian principals to control military affairs under crisis conditions?
- What role can IO play in improving international crisis outcomes?

Priority: 3
Key Terms: IO, IW, Crisis management, deterrence, escalation

6.8 Review and analyze rules of engagement (ROE)/Laws of Armed Conflict (LOAC) for offensive IW.

- How do LOAC apply, especially in relation to effect on civilians?
- How do LOAC concepts, such as "proportionality," "collateral damage," "humanity," "chivalry," apply in the context of offensive IW?
- What ROE issues must be considered during a conflict that contains a technology-based IW component?
- How should we devise effective ROE to respond to cyber-attack?

Priority: 3
Key Terms: IO, IW, LOAC, ROE, operations, operational law

6.9 Discuss the similarities and differences between Joint and Air Force IO doctrine, and how the organizational structures interface?

- Air Force doctrine diverges from Joint doctrine. Has this divergence helped or hurt IO efforts in the Air Force and in the Joint arena? Examine recent/current operations to help answer this question.
- Examine utility of Information in Warfare construct. Is there any utility of distinguishing IO and IW based upon conflict vs. non-conflict timelines?

- Discuss the nature of confusion due to lexicon differences and its effect on the US, its allies and its adversaries.
- How do organizations that utilize both doctrines cope with the differences? Again, examine current conflicts and/or Joint exercises to help answer this question.

Priority: 3
Key Terms: IO, IW, Doctrine

OPERATIONS ISSUES

6.10 What unintended consequences (or "blowback") could result from the employment of computer network attacks (CNA)?

- Would the purported deniability or non-traceability of electronic attacks prevent attacked societies from focusing on the originating country or group?
- Just as traditional US military capabilities have shown a clear progression away from mass effects against societies and toward precision effects against military capabilities, should IW policy and capabilities, if/when developed, focus on precision rather than mass information effects?
- What is the effect of large-scale CNAs that address civilian infrastructure and defense issues? What are the policy issues associated with these various scenarios?
- How does the unpredictability of the "weapon" create law of armed conflict (LOAC) issues?

Priority: 1
Key Terms: IO, IW, LOAC, law of armed conflict, unintended consequences, policy issues, CNA, blowback

6.11 How can we improve IO in a coalition/allied environment?

- How do security concerns and improved technologies impact IO in a coalition/allied environment? What do/don't we share or disclose? How do we overcome these concerns? How does this issue relate to homeland defense?
- Do current Concepts of Operations need to be changed? How?
- How have allies such as the UK or NATO handled IO better? Examine the concept operations for allied Public Information Officers in relation to US Public Affairs Officers.
- Analyze real world and exercise examples of successes and failures of IO operating in a coalition/allied effort.

Priority: 1
Key Terms: IO, IW, coalition, security, homeland defense

6.12 How do we measure nation-states'/non-state entities' levels of vulnerability to IW?

- What are measures of effectiveness (MOE) in an IW campaign? Which elements of IW can be quantified via MOE?
- Does the US do too much "mirror-imaging"? What models can be used to avoid errors made my mirror-imaging?
- Examine portions of a potential adversary's infrastructure. Include insights on why categories were chosen, application to other analysis, and potential interrelationships between categories.
- How do we determine the key nodes/centers of gravity (COGs) in an adversary's information infrastructure? What models are useful in determining nodes/COGs for Influence Operations?

Priority: 1
Key Terms: IO, IW, vulnerability, mirror imaging, infrastructure, COG, targeting, Influence Operations

6.13 What are measures of effectiveness (MOEs) for IW, or one of its disciplines?

- What are ways to measure IW contributions in terms of denying data, information, knowledge, understanding, and operational wisdom?
- How can the Unified Joint Task List (UJTL) MOEs be used as a foundation for more sophisticated MOE development?
- Can Joint Munitions Effectiveness Manuals (JMEMs) be developed for IW?
- What do commanders expect of IW and how can those expectations be measured?
- How can IW MOEs be validated?
- What are some MOE categories (e.g., planning process, programmatic, logistical, time, damage, perception management, etc.)?
- What are ways to conduct IW combat assessment (like battle damage assessment)?

Priority: 1
Key Terms: IO, IW, measures of effectiveness, Universal Joint Task List

6.14 What is the effect of international media on US military operations and on IW/IO planning?

- Citing case studies as examples, discuss which IW/IO means were most important for a given side in a particular conflict.
- How should the AF and DOD implement the provisions of PDD-68
- How should the AF and DOD provide international public information?

Priority: 1
Key Terms: IO, IW, media, IO planning, Kosovo, Serbia, Afghanistan, Iraq

6.15 What is the interrelationship of themes between Public Affairs (PA), Psychological Operations (PSYOP), and Military Deception (MD)?

- In an Information Warfare Flight or a Joint Force Commander IO Cell how are PA, PSYOP and MD themes coordinated and deconflicted effectively?
- What is a workable definition of Influence Operations?
- Who are the key audiences for PA, PSYOP and MD? Is there a concept of acceptable collateral (media) damage if a message is received by the wrong audience?
- How can PA maintain "integrity and credibility" while working with PSYOP and MD?
- Discuss the separation between Public Affairs (counter-propaganda) aimed at a US audience vs. activities directed at foreign and/or hostile audiences.
- What is the advantage gained by combining PA, PSYOP, MD and OPSEC under a coordinated planning effort?
- What are the lessons learned from post 9/11 experiences in Afghanistan or Iraq that support

Priority: 1
Key Terms: IO, IW, deception, PSYOP, propaganda, public affairs, media, international

6.16 Are Effects-Based Operations (EBO) another name for Command and Control Warfare (C2W) or Influence Operations?

- What new concepts to Information Warfare (IW) are brought to the table by EBO not already part of the definition of C2W and nodal targeting or current AF/Joint concepts of IW?
- How do you categorize lethal and non-lethal weapons and kinetic/non-kinetic effects in relation to EBO?
- Analyze AFDD 2-1.9, AF Targeting Doctrine, in relation to EBO and IW effects.
- EBO have been defined as "coordinated sets of actions directed at shaping the behavior of friends, neutrals, and foes in peace, crisis, and war. What are the differences/similarities from 'Influence Operations' under consideration for inclusion in DoDD 3600.1, JP 3-13 and AFDD 2-5?
- Are Information Operations required as a separate planning function if all operations are planned with vertical and horizontal integration of Effects-Based Operations?

Priority: 2
Key Terms: IO, IW, EBO, C2W, Targeting, Influence Operations

6.17 How does IW contribute to full-dimensional force protection (critical nodes of personnel, facilities, equipment and technologies)?

- What new critical infrastructure protection processes/procedures/measures need to be introduced to counter the possibility of hostile activity?
- What IW-related analytical or decision-making tools does the air commander require to ensure force protection?

- What commercial off-the-shelf (COTS) or emerging technologies, media resources, and human factors analysis would enhance force protection efforts?

Priority: 2
Key Terms: IO, IW, force protection, COTS, human factors, media

6.18 What tools do commanders need to conduct IW at each level (IW Flight/CC, JTF, CINC)?

- How are the tools linked together? How could/should other links be made?
- Discern commanders' requirements for automated or semi-automated IW mission planning tools and common operating pictures (COPs).
- What tools would help ensure that the commander is considering all targeting options (kinetic/nonkinetic, lethal/nonlethal)?
- How can advanced technology, human factors, and human computer interaction understanding be used to enhance these tools?
- How can the need for these tools be translated into operational and acquisition requirements?
- How can education and training programs be used to effectively integrate these tools with force protection and other related base operations?
- How can visualization of IO/IW activities be most usefully integrated with other information presented to the commander?
- What measures of effectiveness would be embedded in such a visualization/map?

Priority: 2
Key Terms: IO, IW, mission planning, targeting

6.19 How can Psychological Operations (PSYOP) be used most effectively in support of air and space activities?

- What does psychological preparation of the battlespace (P2B) entail, from both an operational and conceptual standpoint? How should P2B be conducted at the strategic, operational, and tactical levels?
- How can PSYOP be folded into the target development and selection process in support of joint or combined air combat operations? How does PSYOP fit into the effects-based operational framework? What is the Air Force role in the JPOTF of tomorrow?
- What role(s) should PSYOP expeditionary teams (PETs) play during air contingencies and EAF deployments?
- What is the synergy between PSYOP and DOD Influence Operations activities (e.g., public/civil affairs)? How can this synergy best be achieved and optimized?
- What is the synergy between PSYOP and human-factors analysis? How can this synergy best be achieved and optimized? What commercial off-the-shelf (COTS) or emerging technologies could be harnessed to enhance DOD's PSYOP capability?

Priority: 2

Key Terms: IO, IW, aerospace PSYOP, P2B, PETs, human factor analysis, COTS, Influence Operations

6.20 What should the role of public affairs (PA) be in IW?

- The Air Force Chief of Staff has directed PA participation in IW Flights (IWF). What role should PA have in these Flights?
- How will PA contribute to the synergism of IW?
- Examine PA/Command IW relationships.
- What type of "public affairs strategy" should we pursue in respect to defending the national infrastructure, DOD and AF against potential IW attacks?
- What type of public affairs strategy should be created to educate the public in the consequences of attack? Examples might include: crashing the FAA air traffic control network (possibly bringing down airliners filled with innocent civilians); shutting down the US power grid (causing civilian casualties); interfering with 911 networks, sending emergency vehicles to the wrong locations?
- What is the role of AF public affairs in cases where general attacks against civilian infrastructure impacts AF operations?

Priority: 2
Key Terms: IO, IW, public affairs, PSYOP, information infrastructure

6.21 How will continuing rapid changes in technology affect IW?

- How will changes in global telecommunications, embedded devices, increasing bandwidth, etc., affect the use of IW by potential adversaries?
- How will the increasing pace of technological change affect our ability to defend against IW? How should these improved technologies be used in conjunction with our allies? What concerns exist regarding foreign military sales or the possible compromise of technology?
- Bandwidth limitations have traditionally constrained information delivery to warfighters. With increasing bandwidth available, what useful information should be added and what are ideas for displaying information more intuitively? Should some of the new bandwidth be spent to strengthen encryption?

Priority: 3
Key Terms: IO, IW, advanced technology, technology forecasts, technology

6.22 How will continuing rapid changes in human factors analysis affect IW?

- How can new precision profiling techniques, including speech pattern analysis, lie detection, etc., be used in deception and psychological operations campaigns?
- How can cultural studies assist IO campaigns?
- Address the use of human conditioning for exploitation of EW, CNA, OPSEC.

Priority: 3

Key Terms: IO, IW, human factors analysis, behavioral analysis, EW, PSYOP

6.23 What constitutes a complete IW campaign? For us and/or against us?

- Does IO/IW conditioning of adversaries and allies improve the pre-hostilities environment?
- Is it possible to determine specific start and stop dates, or is IW continuous?
- How is the end-state defined in an IW campaign?
- Should there be an IW task force set up?
- What are the phases of an IW campaign? Where do they synchronize with conflict operations?

Priority: 3
Key Terms: IO, IW, campaign end, end state, task force

6.24 Examine the role of maneuver in cyberspace.

- By changing addressing schemes, communications protocols, and their means, the cyberspace location of assets can be changed. Such changes offer the opportunity for maneuver in cyberwarfare.
- How can maneuver concepts improve AF/DOD ability to conduct computer network defense (CND)?
- How can one measure the disruptive effects of defensive maneuver on AF/DOD ability to communicate?
- How do maneuver concepts in cyberspace relate to those in other realms?

Priority: 3
Key Terms: IO, IW, cyberspace, maneuver, space

6.25 How can the USAF IO and information technology capabilities be applied best in environments associated with Military Operations Other than War (MOOTW) or small-scale conflicts (SSC)?

- Apply real world case studies and multiple analytic approaches in addressing this issue. Address successes and failures as appropriate.
- Do our current TTPs, CONOPS, etc., correctly address how we should apply IW during conflict?

Priority: 3
Key Terms: IO, IW, MOOTW, SSC, Kosovo, aerospace power, Mogadishu, Afghanistan

6.26 How can the Air Force develop PSYOP capabilities and integrate them into a Joint IO environment?

- What is the best means for the AF to ensure JPOTF takes Air-centric IO/PSYOP requirements (themes) into consideration?

- How can Commando Solo be better utilized as a non-SOF IO platform vs. a SOF PSYOP platform?
- What AF educational requirements can be created to ensure better PSYOP and Joint integration?

Priority: 3
Key Terms: IO, IW, PSYOP, JPOTF, Commando Solo, education

6.27 Compare Economic, Political, and Religious media reports in the Western and Muslim media. Can the Muslim Arab/Arab media be useful to in supporting US policies and objectives?

- Compare Arab Arab/Muslim media reaction to critical US policy/strategy plans.
- What have been the repercussions of US reactive responses to Arab/Muslim media?
- Compare the credibility and effectiveness of Muslim media with the regional audience, the US audience, and the world audience.
- Can US media be a positive force in Arab/Muslim relations?
- Would Arab/Muslim lead reporters and anchors improve the US image and assist US objectives?
- How do AF efforts fit in with DOD and national efforts to conduct international public information efforts and ensure national will in support of USG policies and objectives?
- How do AF commanders use public affairs and linkages to IW capabilities to negate or mitigate the negative impact of adversary propaganda on AF personnel?

Priority: 3
Key Terms: IO, IW, propaganda, public affairs, international

Defense Operations Issues

6.28 How should IW address the risk management issue for IO preparation of the battlespace (IOPB)?

- Is risk management properly addressed in current IW TTPs? What changes if any are needed?
- How do we determine the level of acceptable risk?
- Are current Multidisciplinary Vulnerability Assessments (MDVA) acceptable tests to determine if risk management procedures are appropriate?
- Do the Operational Risk Management procedures used to design the INFOCON process also apply to the other disciplines of defensive counter information?

Priority: 2
Key Terms: IO, IW, defensive counter-information, risk management, IO vulnerabilities, TTPs, operational planning, Multidisciplinary Vulnerability Assessments, IOPB

6.29 Explore concept of computer network exploitation (CNE)/"Active Defense."

- Define concept of CNE/"active defense" in cyber-warfare and how it is distinguished from related CND, Computer Network Attack (CNA), and Info Assurance activities.
- What advantages does having authorization and capability to conduct CNE/"active defense" as part of CND provide? What are the implications of not having authority?
- What policy and legal considerations apply to CNE/"active defense" and the establishment of ROE for its prosecution?

Priority: 2
Key Terms: IO, IW, CNE, active defense, legal, cyber-warfare

6.30 What are the ramifications of hostile IO/IW threats to the US, its forces, and allies?

- Analysis of key strategic and operational IW threats to the US past and present.
- Include nation-state and non-state-entity operations.
- Possible deterrence of such activity.
- Future implications.
- Include case studies.

Priority: 2
Key Terms: IO, IW, deterrence, anti-US, political-military, public diplomacy, terrorism

6.31 What lessons can be learned from the private sector regarding defensive IW?

- What are the similarities and differences in the challenge of protecting the information resources of globally dispersed operations?
- How does a large, geographically dispersed organization identify, protect, and defend its most critical information assets?
- What is the best mix of centralized/decentralized protection and reserve/backup paths and systems in defending the most critical information assets?

Priority: 3
Key Terms: IO, IW, defensive IW, lessons learned, private sector, commercial

6.32 Compare and contrast TTPs for IO/IW across the Services and Joint community.

- Address best practices for the Joint community
- Identify the cross-Service synergies.
- Are the TTPs deconflicted?
- Recommended changes for any/all TTPs.
- Are the JULLS appropriately applied during exercises, contingency operations, in TTP development, and in IO/IW execution?

Priority: 3
Key Terms: IO, IW, TTPs, JULLS, Joint

(NOTE: Research of this topic may require the use of classified sources.)

6.33 How can DOD and the Air Force go beyond computer-focus within the Information Condition (INFOCON) system to a full-spectrum IW focus?

- Is it possible to broaden scope so widely?
- What is the utility of moving to a full-spectrum focus?
- What organizational relationships need to be formed to make this happen?
- What are the necessary reporting chains and means to ensure compliance?
- What indications and warning data are necessary to expand to a full-spectrum threat condition?

Priority: 3
Key Terms: IO, IW, INFOCON

Organizational Issues

6.34 How can you build an IW capable force?

- Examine total force capabilities.
- Should a person be trained in all aspects of IW or should they specialize?
- Should we train to Joint or Service standards/doctrine?

Priority: 2
Key Terms: IO, IW, information warrior, standards, training, entrance testing and exams, AFSCs, Air Force Reserves (AFR), Air National Guard (ANG), ARC

6.35 Examine the possible roles and responsibilities of Air National Guard and Air Force Reserve units in IO.

- What IO roles and missions should the reserve components assume? (Include homeland defense missions in the analysis.)
- What units might be formed or slots created which will enable the United States to better utilize its IO-trained resources?
- How can their capabilities be better integrated into Total Force capabilities?

Priority: 2
Key Terms: IO, IW, Air National Guard, ARC, Reserve, National Guard

6.36 IO is conducted in a distinct battlespace. What type of organizational structure is best suited to accomplish the IO mission?

- Who should have the national IO lead?
- How do you best integrate and synchronize the diplomatic, informational, military, and economic (DIME) aspects?

- How does the Interagency Working Group structure feed the Joint Force Commander IO Cell? How does it feed Strategic Command?
- Should there be a new model for conducting IO, such as an "IO Combatant Commander," MAJCOM, or IO Task Force? What roles would each organization have? What should the organization look like?
- How does Strategic Command conduct command and control of IO? Who has the decision authority for CNA, PSYOP, and Special Information Operations? How does this organization interact with the Services? What would be their individual responsibilities?

Priority: 2
Key Terms: IO, IW, force structure, information infrastructure, C2, command and control, Strategic Command

6.37 CORONA 98 established AF Information Warfare Flights (IWFs) at Numbered Air Forces in order to provide IW support to the NAF Commander. Currently, CORONA-directed IWFs exist at 7AF, 8AF, 9AF, 12AF, PACAF, and USAFE and are AOR-oriented. HQ USAF/XOI approved additional functionally-oriented IWFs at 1AF, 14AF, AMC. What has been the overall effectiveness of each IWF, as judged by their supported command, since their inception?

- Is the IWF the best way to leverage IO capabilities in a given theater?
- Do all IWFs have enough unique mission to justify their funding, staffing and existence?
- If IWFs are deemed necessary, do IWFs require specified AF training, or could already existing joint IO training suffice?
- What is the relationship between the IWFs and Joint IO organizations?
- Could the current IWF tasks be better accomplished via Joint IO organizations?
- When deployed in support of operations, what is the best way to leverage IO capabilities?

Priority: 2
Key Terms: IO, IW, IWF, organization

6.38 What role is assigned to Network Operations Security Center (NOSC) personnel embedded in the Information Warfare Flight or within the Information Warfare Team within the Air Operations Center (AOC)?

- How does the NOSC insert within the Air Operations Center (Falconer AOC manning) interface with the Air Force Computer Emergency Response Team (AFCERT)? Is there a better construct than embedding NOSC trained personnel with the IW Team?
- What is the NOSC insert/AOC interface with the Joint IO Cell and Joint Task Force-Computer Network Operations?

- Analyze the AF role in protecting the United States National Information Infrastructure (NII).

Priority: 3
Key Terms: IO, IW, NII, Defending America's Cyberspace, homeland defense, AOC